Reuben D. Nathan, Esq. (SBN 208436)
NATHAN & ASSOCIATES, APC
2901 W. Coast Hwy., Suite 200
Newport Beach, CA 92663
Office: (949) 270-2798
Email: rnathan@nathanlawpractice.com

Ross Cornell, Esq. (SBN 210413)
LAW OFFICES OF ROSS CORNELL, APC
40729 Village Dr., Suite 8 - 1989
Big Bear Lake, CA 92315
Office: (562) 612-1708
Email: rc@rosscornelllaw.com

Attorneys for Plaintiff: JOHN JANIGA

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JOHN JANIGA, on behalf of himself and all similarly situated persons, Plaintiff, v. STUBHUB, INC., a Delaware corporation, Defendants.	Case No: **COMPLAINT** 1. Cal. Penal Code § 638.51 2. Cal. Bus. & Prof. Code § 17200, *et seq.* **CLASS ACTION**

I. NATURE OF THE ACTION

1. Defendant STUBHUB, INC., a Delaware corporation (referred to herein as "Defendant" or "STUBHUB") own and operate a website, www.stubhub.com (the "Website").

2. This is a class action lawsuit brought by Plaintiff on behalf of himself and on behalf of all California residents who have accessed the Website.

3. Plaintiff JOHN JANIGA files this class action complaint on behalf of himself and all others similarly situated (the "Class Members") against Defendant. Plaintiff brings this action based upon personal knowledge of the facts pertaining to him, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

4. A pixel tracker, also known as a web beacon, is a tracking mechanism embedded in a website that monitors user interactions. It typically appears as a small, transparent 1x1 image or a lightweight JavaScript snippet that activates when a webpage is loaded or a user performs a tracked action.

5. When triggered, the pixel transmits data from the user's browser to a third-party server. This data typically includes page views, session duration, referrer URLs, IP address, browser and device details, and other interaction metadata.

6. When users visit the Website, Defendant causes tracking technologies to be installed, executed, embedded, or injected in visitors' browsers. These include, but are not limited to, the following:

- Google Ads/DoubleClick Tracker
- Microsoft Bing Ads Tracker
- Branch.io Tracker
- Viagogo Tracker

7. The third parties who operate the above-listed trackers use pieces of User Information (defined below) collected via the Website as described herein for their own independent purposes tied to broader advertising ecosystems, profiling, and data

monetization strategies that go beyond Defendant's direct needs for their own financial gain. The above-listed trackers are referred to herein collectively as the "Trackers."

8. The Trackers are operated by distinct third-party entities: Google LLC (Google Ads / DoubleClick Tracker), Microsoft Corporation (Microsoft Bing Ads Tracker), Branch Metrics, Inc. (Branch.io Tracker), and Viagogo Entertainment Inc. (Viagogo Tracker). The defendant enables these trackers, which transmit user data to servers controlled by the respective third parties. This transmission allows for the identification of users and supports various activities such as targeted advertising, user profiling, cross-site tracking, and the monetization of personal information.

9. Through the Trackers, the Third Parties collect detailed user information including IP addresses, browser and device type, screen resolution, operating system, pages visited, session duration, scroll depth, mouse movements, click behavior, referring URLs, unique identifiers (such as cookies and ad IDs), and geolocation based on IP. This information is used for behavioral profiling, ad targeting, cross-device tracking, and participation in real-time advertising auctions (collectively, "User Information").

10. Because the Trackers capture and transmit users' IP addresses, full page URLs, referrer headers, device identifiers, and other non-content metadata, they function as "pen registers" and/or "trap and trace devices" under Cal. Penal Code § 638.50. These tools silently collect routing and addressing information for commercial use without user interaction, as defined in *Greenley v. Kochava, Inc.*, 2023 WL 4833466 (S.D. Cal. July 27, 2023).

11. Plaintiff and the Class Members did not consent to the installation, execution, embedding, or injection of the Trackers on their devices and did not expect their behavioral data to be disclosed or monetized in this way. By installing and using the Trackers without prior consent and without a court order, Defendant violated CIPA section 638.51.

/ /

12. By installing and activating the Trackers without obtaining user consent or a valid court order, Defendant violated California Penal Code § 638.51, which prohibits the use of pen registers and trap and trace devices under these circumstances.

13. Defendant provides a privacy policy referred to as "User Privacy Notice" on the Website (the "Privacy Policy"). On information and belief, Defendant, by and through the Website, does not conform to the Privacy Policy:

a. Defendant represents that it engages third-party companies and individuals to help operate, provide, and advertise its services and that such third parties have limited access to personal information and are only permitted to use personal information to perform the identified tasks on Defendant's behalf and are prohibited from disclosing or using personal information for other purposes. Defendant claims limited, purpose-bound sharing, which is inconsistent with the broad dissemination of tracking data to third-party adtech ecosystems with no indication of real-time constraint enforcement.

b. Defendant does not clearly disclose that real-time behavioral data is transmitted to third parties immediately upon site arrival;

c. Defendant represents that the Website uses data analytics software to improve its services and that Defendant relies on consumer consent to personalize advertisements on third-party platforms. In reality, the Website provides no initial consent mechanism;

d. Tracking and third-party sharing occurs prior to presenting users with a valid choice to opt-out or manage consent;

e. Defendant omits material details regarding the depth of personal data shared with third parties and the nature of behavioral profiling activities.

/ /

14. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of California residents.

15. Generalized references herein to users, visitors and consumers expressly include Plaintiff and the Class Members.

II. PARTIES

16. Plaintiff JOHN JANIGA ("Plaintiff") is a California citizen residing in San Bernardino County and has an intent to remain there. Plaintiff was in California when he visited the Website, which occurred during the class period prior to the filing of the complaint in this matter including but not limited to April 28, 2025. The allegations set forth herein are based on the Website as configured when Plaintiff visited it.

17. Defendant STUBHUB, INC. is a Delaware corporation that owns, operates and/or controls the Website which is an online platform that offers goods and services to consumers.

18. STUBHUB is a prominent online ticket marketplace specializing in the resale of live event tickets for concerts, sports, theater, and other entertainment experiences. The company maintains a substantial digital presence in the United States and operates its primary consumer platform at www.stubhub.com. STUBHUB enables users to browse, purchase, and resell tickets for thousands of events across the globe, connecting buyers and sellers through a centralized and user friendly platform.

19. STUBHUB functions as the flagship consumer facing brand of STUBHUB's broader event ticketing and resale infrastructure. While the company offers a range of tools for both casual sellers and professional brokers, the STUBHUB Website platform is directly responsible for facilitating ticket transactions, processing payments, and managing communications between parties. In the course of operating its ticket marketplace, STUBHUB collects and processes substantial volumes of consumer data for purposes including transaction processing, behavioral analysis, targeted marketing, and affiliate network operations.

20. The Website serves as STUBHUB's primary digital storefront, enabling users to search for events, manage ticket listings, access customer accounts, and complete transactions. Beyond these consumer facing features, the Website also operates as a sophisticated behavioral tracking and digital advertising platform. Through the integration of third party tracking technologies including advertising pixels, event trackers, behavioral analytics scripts, and data exchange tools, STUBHUB systematically captures detailed information about user activity and preferences. These data collection practices are central to STUBHUB's performance marketing, ad targeting, and user segmentation strategies.

III. JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the total matter in controversy exceeds $5,000,000 and there are over 100 members of the proposed class. Further, at least one member of the proposed class is a citizen of a State within the United States and at least one defendant is the citizen or subject of a foreign state.

22. This Court has personal jurisdiction over Defendant because, on information and belief, Defendant has purposefully directed its activities to the Central District of California by regularly engaging with individuals in California through its website. Defendant's illegal conduct is directed at and harms California residents, including Plaintiff, and if not for Defendant's contact with the forum, Plaintiff would not have suffered harm.

23. Venue is proper in the Central District of California pursuant to 28 U.S.C. § 1391 because Defendant (1) is authorized to conduct business in this District and has intentionally availed itself of the laws and markets within this District; (2) does substantial business within this District; (3) is subject to personal jurisdiction in this District because it has availed itself of the laws and markets within this District; and (4) the injury to Plaintiff occurred within this District.

/ /

IV. GENERAL ALLEGATIONS

1. *The California Invasion of Privacy Act (CIPA)*

24. Enacted in 1967, the California Invasion of Privacy Act (CIPA) is a legislative measure designed to safeguard the privacy rights of California residents by prohibiting unauthorized wiretapping and eavesdropping on private communications. The California Legislature recognized the significant threat posed by emerging surveillance technologies, stating that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society" (Cal. Penal Code § 630).

25. CIPA specifically prohibits the installation or use of "pen registers" and "trap and trace devices" without consent or a court order (Cal. Penal Code § 638.51(a)).

26. A "pen register" is defined as a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, excluding the contents of the communication (Cal. Penal Code § 638.50(b)).

27. Conversely, a "trap and trace device" captures incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, again excluding the contents (Cal. Penal Code § 638.50(b)).

28. In practical terms, a pen register records outgoing dialing information, while a trap and trace device records incoming dialing information.

29. Historically, law enforcement has utilized these devices to monitor telephone calls, with pen registers recording outgoing numbers dialed from a specific line and trap and trace devices recording incoming call numbers to that line.

30. Although originally focused on landline telephone calls, CIPA's scope has expanded to encompass various forms of communication, including cell phones and online interactions. For instance, if a user sends an email, a pen register could record

the sender's email address, the recipient's email address, and the subject line—essentially capturing the user's outgoing information.

31. Similarly, if the user receives an email, a trap and trace device could record the sender's email address, the recipient's email address, and the subject line—capturing the incoming information.

32. Despite predating the Internet, CIPA has been interpreted by the California Supreme Court to apply to new technologies where such application does not conflict with the statutory scheme (*In re Google Inc.*, 2013 WL 5423918, at *21; *Greenley*, supra, 2023 WL 4833466, at *15; *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1). This interpretation aligns with the principle that CIPA should be construed to provide the greatest privacy protection when faced with multiple possible interpretations (*Matera v. Google Inc.*, 2016 WL 8200619, at *19).

33. The conduct alleged herein constitutes a violation of a legally protected privacy interest that is both concrete and particularized. Invasions of privacy have long been actionable under common law. (*Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019); Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017).)

34. Both the legislative history and statutory language indicate that the California Legislature intended CIPA to protect core privacy rights. Courts have found that violations of CIPA give rise to concrete injuries sufficient to confer standing under Article III. (See *Campbell v. Facebook, Inc.*, 2020 WL 1023350; *In re Facebook Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020).)

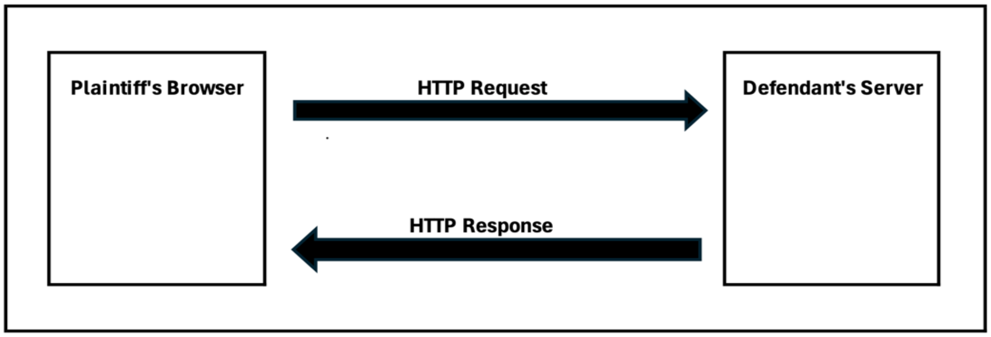
35. Individuals may pursue legal action against violators of any CIPA provision, including Section 638.51, and are entitled to seek $5,000 in statutory penalties per violation (Cal. Penal Code § 637.2(a)(1)).

2. *The Trackers Are "Pen Registers" and/or "Trap and Trace Devices"*

36. When the Plaintiff and Class Members accessed the Website, their browsers initiated an HTTP or HTTPS request to Defendant's web server, which hosts the content and functionality of the site. In response, the server transmitted an HTTP

response containing the necessary resources including HTML, cascading style sheets (CSS), JavaScript files, and image assets used by the browser to render and display the webpage. These resources also included client-side scripts that initiate communication with third-party services for analytics, marketing, and tracking purposes. ***Figure 1*** below illustrates sample HTTP requests.

Figure 1



37. The server's response included third-party tracking scripts that were executed by the Plaintiff's and Class Members' web browsers. These scripts, once executed, initiate client-side functions that capture routing and behavioral metadata and transmit this data typically via HTTPS requests to the servers of third-party tracking vendors. These actions occur without visible indicators or user awareness. The transmitted data, referred to as User Information, included identifiers such as IP addresses, device characteristics, browser types, page navigation behavior, and unique tracking cookies, all of which were used to profile users and facilitate targeted advertising.

38. The Trackers operate by initiating HTTP or HTTPS requests—using either the GET or POST method from the user's browser to external servers controlled by the Third Parties. These requests are triggered automatically during the page load and by user interactions with the Website. They are used to transmit behavioral data and device metadata, including information such as page views, click events, session duration, and identifying browser characteristics.

/ /

39. An Internet Protocol (IP) address is a numerical identifier assigned to each device or network connected to the Internet, used to facilitate communication between systems. *See hiQ Labs, Inc. v. LinkedIn Corp.* (9th Cir. 2019) 938 F.3d 985, 991 n.4. The most common format, known as IPv4, consists of four numbers separated by periods (e.g., 191.145.132.123). IP addresses enable routing of data between devices and can be used via external geolocation services to infer a user's general location, including state, city, and in some cases, ZIP code.

40. Public IP addresses are unique identifiers assigned by Internet Service Providers (ISPs) that allow devices to communicate directly over the Internet. They are globally accessible, meaning they can be reached from anywhere on the Internet, but are not inherently exposed unless data is being transmitted. Public IP addresses are essential for devices requiring direct Internet access and can be used to approximate a device's physical location through geolocation services.

41. In contrast, private IP addresses are used within internal networks and are not routable on the public Internet. They are isolated from the global Internet and can be reused across different networks without conflict. Unlike public IP addresses, private IP addresses do not divulge a user's geolocation.

42. Public IP addresses play a significant role in digital marketing by enabling geographic targeting based on a user's approximate location. Through IP geolocation services, advertisers can often determine a user's country, region, city, and in some cases, ZIP code or service area. In contexts where a static IP address is associated with a fixed residence or business, this data can contribute to household-level or business-level targeting, particularly when combined with other tracking identifiers and third-party enrichment.

43. A public IP address functions as "routing, addressing, or signaling information" by facilitating internet communication. It provides essential information that can help determine the general geographic coordinates of a user accessing a website through geolocation databases. Additionally, a public IP address is involved in routing

communications from the user's router to the intended destination, ensuring that emails, websites, streaming content, and other data reach the user correctly.

44. As "routing, addressing, or signaling information," a public IP address is indispensable for maintaining seamless and efficient communication over the Internet. It ensures that data packets are sent from the user's router to the intended destination, such as a website or email server.

45. Defendant installs Trackers on users' browsers to collect User Information, including IP addresses and full URLs, which constitute outgoing routing and addressing metadata under CIPA. These identifiers serve the same function as telephony dialed numbers and therefore meet the statutory definition of a pen register or trap and trace device.

3. *The Use of Pixel Trackers or Beacons and Digital Fingerprinting*

46. Website users typically expect a degree of anonymity when browsing, particularly when they are not logged into an account. However, upon visiting the Website, Plaintiff's and Class Members' browsers executed third-party tracking scripts embedded by the Defendant. These Trackers operate in the background of the browsing session and collect detailed behavioral and technical information, which is then transmitted to external third-party servers without the users' active awareness.

47. This process, known as digital fingerprinting, involves compiling various data points such as browser version, screen resolution, installed fonts, device type, and language settings to generate a unique identifier for each user. Fingerprinting can be used to recognize repeat visits and correlate activity across different sessions or sites. When combined with form inputs, login activity, or third-party enrichment, fingerprinting can contribute to broader profiling of a user's interests, affiliations, or behaviors.

48. When combined with additional tracking mechanisms such as cookies, login data, and third-party enrichment services, fingerprinting contributes to user profiling. This may include inferring location, browsing habits, consumer preferences,

and potentially associating these patterns with known user identities. A sufficiently detailed digital fingerprint, especially when correlated with other identifiers such as email addresses, form submissions, or third-party databases, can enable the reidentification of a user.

49. The ability to associate a persistent digital profile with a specific individual using techniques such as digital fingerprinting has led to the development of a data industry known as identity resolution. Identity resolution involves recognizing users across sessions, devices, and platforms by connecting various identifiers derived from their digital behavior, including IP addresses, browser metadata, cookies, and, in some cases, login credentials. The process may occur deterministically (based on known logins or user-submitted information) or probabilistically (based on behavioral or technical similarity).

50. In simpler terms, pen register and trap and trace mechanisms in the digital context refer to technologies that record metadata such as IP addresses, URLs visited, and device characteristics, information that identifies the routing and addressing of electronic communications. This can be achieved through the deployment of tracking technologies like the Trackers installed, executed, embedded or injected in the Website, which operate without user interaction or visibility.

51. The Trackers provide analytics and marketing services to Defendant using the data collected from visitors to the Website. These services also leverage user data collected from other websites that include the same pen register and trap and trace devices operated by the Third Parties.

52. When users visit the Website, installed, executed, embedded or injected Trackers initiate network requests to third-party servers, using invisible image pixels, JavaScript calls, or beacon APIs. These requests include the user's IP address, which is transmitted automatically as part of the HTTP request header. In many cases, the Tracker's server responds by placing a persistent cookie in the user's browser, which serves as a unique identifier that can be used to recognize and track the user across

future visits. If a user deletes their browser cookies, this identifier is removed. However, upon revisiting the Website, the process repeats: the browser executes the Tracker's script, a new identifier is set, and the Tracker resumes collecting the user's IP address and associated behavioral data.

4. *Plaintiff's And Class Members' Data Has Financial Value*

53. Given the number of Internet users, the "world's most valuable resource is no longer oil, but data."[1]

54. Consumers' web browsing histories have an economic value more than $52 per year, while their contact information is worth at least $4.20 per year, and their demographic information is worth at least $3.00 per year.[2]

55. There is "a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories."[3]

56. Extracted personal data can be used to design products, platforms, and marketing techniques. A study by the McKinsey global consultancy concluded that businesses that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

57. In 2013, the Organization for Economic Cooperation and Development ("OECD") estimated that data trafficking markets had begun pricing personal data, including those obtained in illicit ways without personal consent. It found that illegal markets in personal data valued each credit cardholder record at between 1 and 30 U.S.

[1] Ian Cohen, Are Web-Tracking Tools Putting Your Company at Risk?, Forbes (Oct 19, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/10/19/are-web-tracking-tools-putting-your-company-atrisk/?sh=26481de07444

[2] *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 928 (N.D. Cal. 2015), rev'd, 956 F.3rd 589 (9th Cir. 2020).

[3] *In re Facebook, Inc. Internet Tracking Litigation* (9th Cir. 2020) 956 F.3rd 589, 600.

[4] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, Capturing value from your customer data, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/businessfunctions/quantumblack/ourinsights/capturing-value-from-your-customer-data

dollars in 2009, while bank account records were valued at up to 850 U.S. dollars. Data brokers sell customer profiles of the sort that an online retailer might collect and maintain for about 55 U.S. dollars, and that individual points of personal data ranged in price from $0.50 cents for an address, $2 for a birthday, $8 for a social security number, $3 for a driver's license number, and $35 for a military record (which includes a birth date, an identification number, a career assignment, height, weight, and other information). Experiments asking individuals in the United States and elsewhere how much they value their personal data points result in estimates of up to $6 for purchasing activity, and $150-240 per credit card number or social security number.[5]

58. The last estimate probably reflects public reporting that identify theft affecting a credit card number or social security number can result in financial losses of up to $10,200 per victim.[6]

59. The Defendant's monetization of personal data constitutes actionable economic harm under federal law, even without evidence of a direct financial loss, as a "misappropriation-like injury" caused by converting user data into a revenue stream through targeted advertising. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020).

5. *Defendant Is Motivated To Monetize Consumer Information Regardless of Consent*

60. Data harvesting is one of the fastest growing industries in the country, with estimates suggesting that internet companies earned $202 per American user in 2018 from mining and selling data. That figure is expected to increase with estimates for 2022 as high as $434 per use, reflecting a more than $200 billion industry.

[5] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220 (Apr. 2, 2013), at 27-28, https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf

[6] Bradley J. Fikes, Identity Theft Hits Millions, Report Says, San Diego Union Tribune, Sept. 4, 2003, https://www.sandiegouniontribune.com/sdut-identity-theft-hits-millions-report-says-2003sep04-story.html.

61. By implementing Trackers on the Website, Defendant participates in building detailed behavioral profiles of visitors. These profiles may include information such as which users viewed specific products, engaged with pages or interface elements, or demonstrated purchase intent. This data enables Defendant and its advertising partners to identify repeat visits from the same device or browser. The behavioral data is integrated into third-party advertising platforms, allowing Defendant to deliver retargeted ads to users who previously visited the Website, offer promotional incentives to re-engage high-intent visitors, and build “lookalike audiences” that target users with similar behaviors or characteristics. These practices significantly improve advertising efficiency and increase the likelihood of converting user engagement into actual sales.

62. Defendant has a strong financial incentive to deploy the Trackers on its Website without obtaining user consent. By enabling the collection of IP addresses and device-level identifiers through these technologies, Defendant facilitates integration into real-time bidding ecosystems. These systems rely on bidstream data such as IP address, device type, screen resolution, and referral information to assess the value of a potential ad impression. This enables Defendant and its partners to participate in data-driven ad targeting, increase the value of its advertising inventory, and track users across sessions and websites, all of which provide economic benefit despite private implications to users.

63. IP addresses are a valuable data point in digital advertising and tracking systems. They can be used to approximate a user’s geographic location, often down to the city or ZIP code level, enabling location-based targeting. When combined with cookies, browser metadata, and device identifiers, IP addresses contribute to persistent user tracking across sessions and websites. They also assist advertisers and data brokers in linking anonymous browsing activity to existing user profiles, which enhances ad targeting precision and increases the commercial value of each tracked interaction. IP addresses therefore constitute “routing, addressing, or signaling information” protected under CIPA § 638.50(b).

64. When users' data is collected without meaningful consent and monetized, they lose control over who can access, use, or distribute their personal information. Data brokers and ad tech firms aggregate and correlate identifiers such as IP addresses, device IDs, and cookies with other personal data to construct detailed consumer profiles. Information initially gathered in one context, such as browsing a retail website, is frequently repurposed for unrelated uses and sold to third parties without the user's awareness. This results in pervasive surveillance, where users are continuously tracked across multiple websites, applications, and devices, often without their knowledge or ability to opt out.

6. *The Trackers Function Together to Achieve Targeted Objectives*

65. When a user visits the Website, a suite of background tracking technologies is activated immediately upon page load. These include client-side scripts deployed by third-party Trackers, which begin collecting various categories of User Information without any visible indication to the user. Together, these technologies function as a coordinated data collection infrastructure that allows Defendant to analyze user behavior at a highly granular level and to leverage that insight in real time for marketing optimization, user targeting, and business intelligence.

66. On information and belief, the Trackers operate as part of a vast and interconnected digital advertising ecosystem, and these entities leverage shared identifiers, cookie syncing, and cross-device tracking techniques to follow users across websites, platforms, and environments, with tools specifically engineered to build persistent consumer profiles, enabling real-time behavioral targeting and identity resolution at scale.

67. On the Website, a coordinated network of third party trackers is deployed to support identity resolution, targeted advertising, and cross platform attribution. This infrastructure includes technologies embedded directly into the Website's source code as well as others activated through JavaScript execution during runtime. The Google Ads and DoubleClick Tracker, Microsoft Bing Ads Tracker, and Viagogo Tracker are

present in the initial page source and activate immediately when the Website loads. The Branch.io Tracker is injected dynamically via JavaScript and begins executing shortly after the initial page load. These trackers operate in tandem to collect real time data about user behavior, device characteristics, and session activity, transmitting that information to external servers for marketing and analytics purposes.

68. Identity resolution on the Website is primarily facilitated through the Viagogo Tracker and the Branch.io Tracker. The Viagogo Tracker allows STUBHUB to correlate on site behavior with user activity across affiliated Viagogo properties, enabling persistent user recognition across domains. The Branch.io Tracker is designed to track referral sources, link navigation, and user flows, creating unified user identities across devices and sessions. These tools help STUBHUB associate browsing activity with individual users over time and support segmentation into behavioral and marketing categories based on observed interaction patterns.

69. Following the collection of identity related data, targeted advertising and user monetization are conducted through platforms such as Google Ads and DoubleClick, as well as Microsoft Bing Ads. Google Ads and DoubleClick use data related to user navigation, click history, and inferred interests to deliver tailored advertisements through automated systems. Microsoft Bing Ads similarly relies on event level data and conversion tracking to drive remarketing efforts and optimize ad performance across Microsoft’s advertising network. These advertising platforms participate in real time bidding ecosystems that allow STUBHUB to auction ad space and user access based on behavioral and demographic indicators, turning Website activity into monetizable advertising opportunities.

70. STUBHUB transmits user data to third party advertising platforms including DoubleClick and Microsoft Bing Ads. These platforms operate real time bidding mechanisms that utilize user behavior data collected during Website visits to inform ad placement decisions. When a user visits the Website, data such as the user’s IP address, browser details, device specifications, and the specific URL visited is

automatically shared with these platforms without any affirmative action or consent from the user. This data enables external advertisers to track users across websites, build behavioral profiles, and deliver interest based advertising in real time.

71. Network traffic directed to endpoints associated with DoubleClick and Microsoft Bing Ads confirms STUBHUB's participation in an advertising architecture built on real time data exchange and user profiling. These systems allow advertisers to bid for ad impressions based on the individual characteristics of each Website visitor, thereby increasing STUBHUB's advertising revenue. These tracking processes serve no functional purpose for the user and exist solely to facilitate the commercial exploitation of user attention. By embedding these technologies to operate immediately and silently upon page load, STUBHUB treats user data as a marketable asset to be leveraged for advertising returns.

V. SPECIFIC ALLEGATIONS

1. Google Ads / DoubleClick Tracker

72. The Google Ads / DoubleClick Tracker is a digital advertising, behavioral tracking, and data brokering technology operated by Google LLC. It is designed to deliver display advertisements, measure engagement, and support real-time bidding on programmatic ad exchanges. The Google Ads / DoubleClick Tracker enables Google and its advertising clients to collect detailed user interaction data and optimize ad delivery across a vast network of third-party websites.

73. When implemented on the Website, the Google Ads / DoubleClick Tracker collects a broad set of user metadata, including visited URLs, session timestamps, referrer headers, and in-page activity data such as page views and navigation events. It also captures technical device attributes such as IP address, screen resolution, browser type, operating system, and language settings. These data points are linked to persistent browser identifiers placed via cookies or pixel fires that allow Google to track users across multiple websites, sessions, and devices, forming longitudinal behavioral profiles. The Google Ads / DoubleClick Tracker also transmits

conversion tracking signals and remarketing data, enabling Google to associate Website interactions with ad conversion events and to retarget users across its advertising ecosystem.

74. The Google Ads / DoubleClick Tracker facilitates monitoring of user activity on the Website, including the capture of pageview events and other engagement signals that can be used to track user progression through various transactional flows. These interaction signals are transmitted to Google's ad infrastructure to facilitate targeted advertising, audience retargeting, and conversion tracking. The Google Ads / DoubleClick Tracker executes via JavaScript calls to domains including googleads.g.doubleclick.net and activates automatically upon page load without requiring any action by the user.

75. ***Figure 2*** below is a screenshot from the Website, showing that a request to googleads.g.doubleclick.net was initiated immediately upon loading the homepage. DevTools confirms a GET request was fired during the initial page load, indicating that the Google Ads / DoubleClick Tracker was activated automatically without any user interaction. The purpose of this outbound request is to transmit data to Google's tracking infrastructure, enabling behavioral profiling and ad delivery. This activity demonstrates that data is sent to Google tracking domains at the moment the Website loads, without any opportunity for user consent or opt-out.

/ /

/ /

/ /

/ /

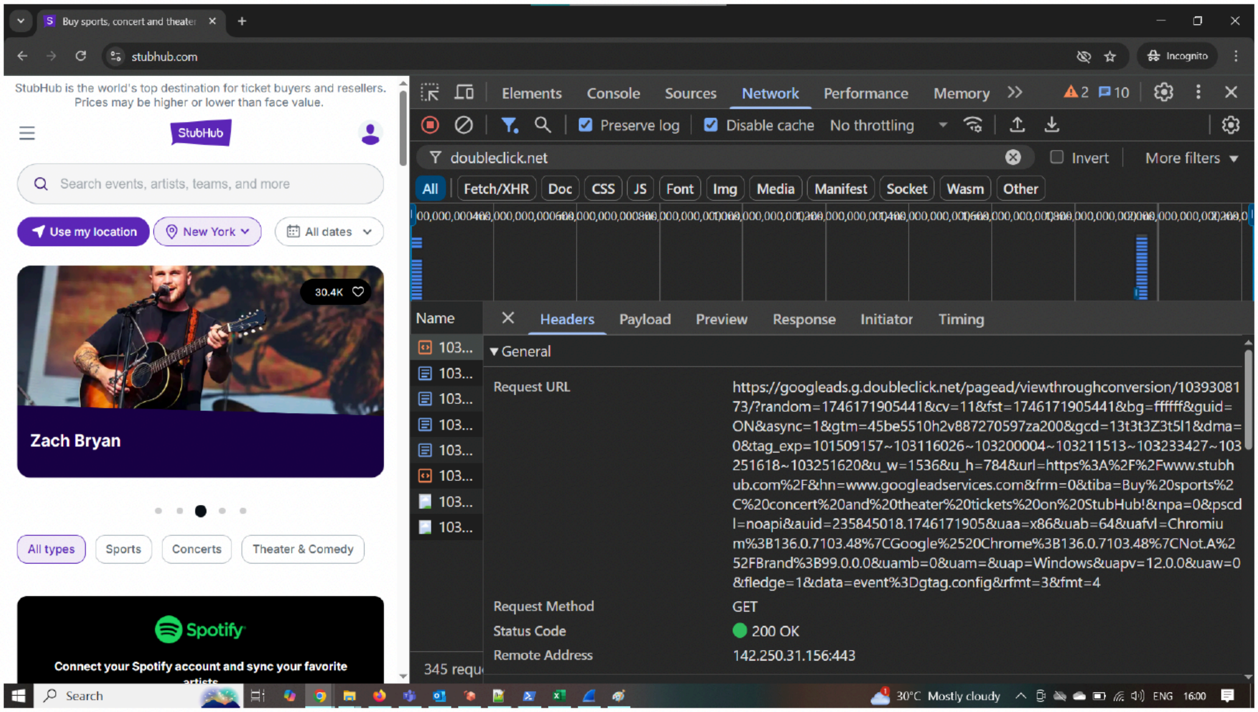
/ /

/ /

/ /

/ /

Figure 2



▾ General

Request URL https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1039308173/?random=1746171905441&cv=11&fst=1746171905441&bg=ffffff&guid=ON&async=1&gtm=45be5510h2v887270597za200&gcd=13t3t3Z3t5l1&dma=0&tag_exp=101509157~103116026~103200004~103211513~103233427~103251618~103251620&u_w=1536&u_h=784&url=https%3A%2F%2Fwww.stubhub.com%2F&hn=www.googleadservices.com&frm=0&tiba=Buy%20sports%2C%20concert%20and%20theater%20tickets%20on%20StubHub!&npa=0&pscdl=noapi&auid=235845018.1746171905&uaa=x86&uab=64&uafvl=Chromium%3B136.0.7103.48%7CGoogle%2520Chrome%3B136.0.7103.48%7CNot.A%252FBrand%3B99.0.0.0&uamb=0&uam=&uap=Windows&uapv=12.0.0&uaw=0&fledge=1&data=event%3Dgtag.config&rfmt=3&fmt=4

Request Method GET

Status Code ● 200 OK

Remote Address 142.250.31.156:443

76. ***Figure 3*** below is a screenshot of network activity on the Website, capturing a request payload transmitted to Google Ads infrastructure during the initial session. The payload includes the client ID, session metadata, and the referrer URL, confirming that identifiable and behavioral information was shared with third parties upon page load. This transmission occurred without any user interaction or consent. The data was sent to subdomains such as googleads.g.doubleclick.net, confirming that the Google Ads / DoubleClick Tracker was silently activated during the initial load of the Website and began transmitting user data immediately.

/ /

/ /

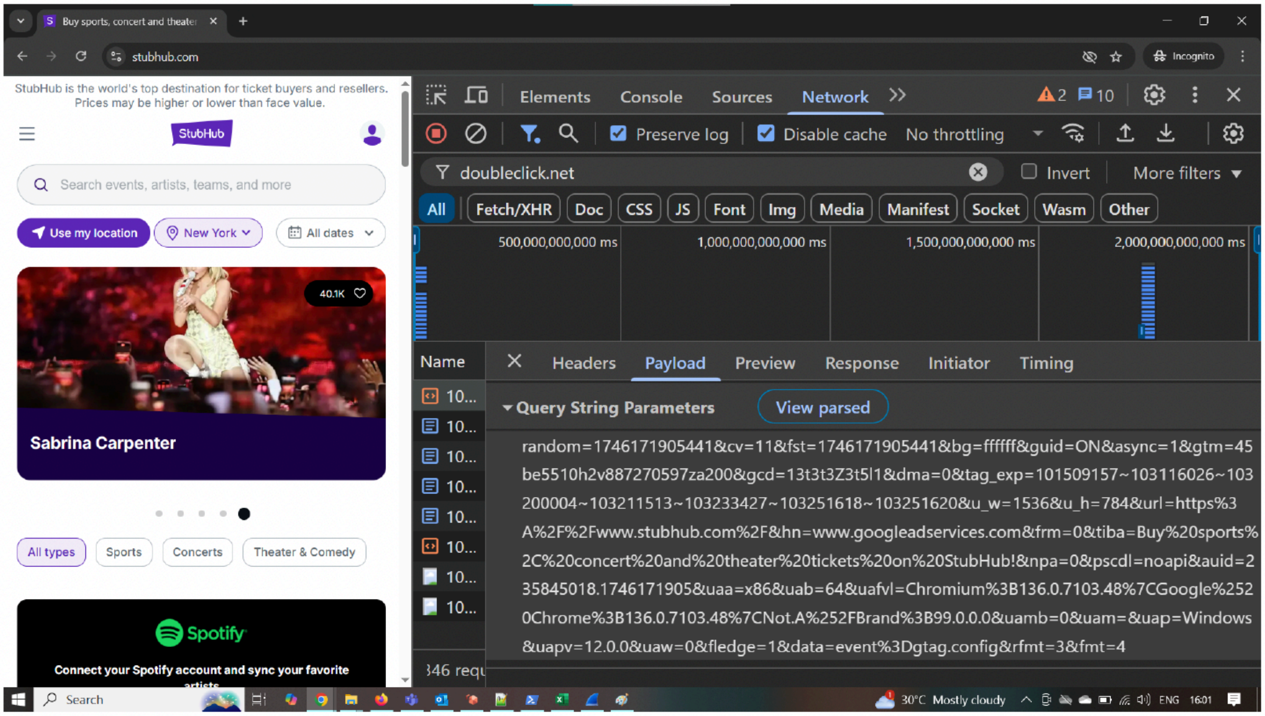
/ /

/ /

/ /

/ /

Figure 3

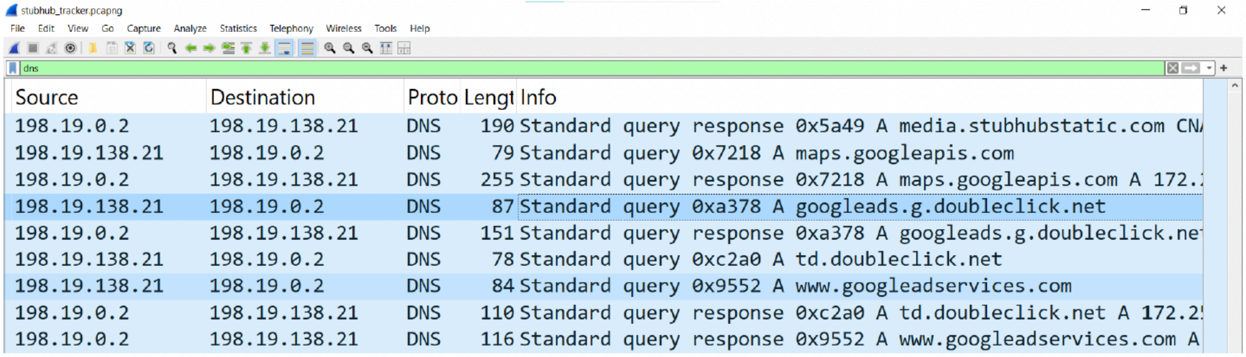


Query String Parameters

```
random=1746171905441&cv=11&fst=1746171905441&bg=ffffff&guid=ON&async=1&gtm=45
be5510h2v887270597za200&gcd=13t3t3Z3t5l1&dma=0&tag_exp=101509157~103116026~103
200004~103211513~103233427~103251618~103251620&u_w=1536&u_h=784&url=https%3
A%2F%2Fwww.stubhub.com%2F&hn=www.googleadservices.com&frm=0&tiba=Buy%20sports%
2C%20concert%20and%20theater%20tickets%20on%20StubHub!&npa=0&pscdl=noapi&auid=2
35845018.1746171905&uaa=x86&uab=64&uafvl=Chromium%3B136.0.7103.48%7CGoogle%252
0Chrome%3B136.0.7103.48%7CNot.A%252FBrand%3B99.0.0.0&uamb=0&uam=&uap=Windows
&uapv=12.0.0&uaw=0&fledge=1&data=event%3Dgtag.config&rfmt=3&fmt=4
```

77. ***Figure 4*** below shows DNS-level network activity captured via Wireshark, confirming that the Website attempted to resolve tracking domains including googleads.g.doubleclick.net and google-analytics.com during the initial session. These DNS queries demonstrate that STUBHUB initiates communication with third-party tracking services as soon as the Website loads, before the user has taken any action or provided consent.

Figure 4



```
Source          Destination     Proto Lengt Info
198.19.0.2      198.19.138.21   DNS     190 Standard query response 0x5a49 A media.stubhubstatic.com CN
198.19.138.21   198.19.0.2      DNS      79 Standard query 0x7218 A maps.googleapis.com
198.19.0.2      198.19.138.21   DNS     255 Standard query response 0x7218 A maps.googleapis.com A 172.
198.19.138.21   198.19.0.2      DNS      87 Standard query 0xa378 A googleads.g.doubleclick.net
198.19.0.2      198.19.138.21   DNS     151 Standard query response 0xa378 A googleads.g.doubleclick.ne
198.19.138.21   198.19.0.2      DNS      78 Standard query 0xc2a0 A td.doubleclick.net
198.19.138.21   198.19.0.2      DNS      84 Standard query 0x9552 A www.googleadservices.com
198.19.0.2      198.19.138.21   DNS     110 Standard query response 0xc2a0 A td.doubleclick.net A 172.2
198.19.0.2      198.19.138.21   DNS     116 Standard query response 0x9552 A www.googleadservices.com A
```

/ /

/ /

78. Defendant surreptitiously installed, executed, embedded or injected the Google Ads / DoubleClick Tracker onto users' browsers by embedding tracking scripts in the Website's page source and by dynamically injecting additional JavaScript tracking code during runtime. When a user visits the Website, their browser automatically executes this code, which initiates outbound network requests to Google's advertising servers and transmits metadata including IP address, page URL, referrer information, device details, behavioral identifiers, and conversion tracking parameters as part of a third-party ad targeting, profiling, and data brokering system.

79. The Google Ads / DoubleClick Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

80. The Google Ads / DoubleClick Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. *See*, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

81. The Google Ads / DoubleClick Tracker functions as a pen register and/or trap and trace device under the California Invasion of Privacy Act because it captures outgoing signaling data such as URLs visited, timestamps, and referrer headers and also processes incoming metadata such as ad impressions and cookie-based session identifiers. These transmissions occur automatically during page load and without user participation, enabling Google to continuously log user behavior and associate it with broader advertising profiles.

82. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Google Ads / DoubleClick Tracker on Plaintiff's and Class Members' browser or to collect or share data with Google.

83. Consequently, the Google Ads / DoubleClick Tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

/ /

2. The Bing / Microsoft Ads Tracker

84. The Bing / Microsoft Ads Tracker, typically delivered through the domain bat.bing.com, is part of the Microsoft Advertising platform (formerly Bing Ads). It is used to track user interactions on websites in order to attribute conversions, retarget visitors, and optimize advertising campaigns across Microsoft's search and display networks, including Bing, MSN, and LinkedIn.

85. The Bing / Microsoft Ads Tracker is designed to silently collect a range of user data when a visitor lands on the Website. It gathers device and browser metadata, IP address, estimated geolocation, referrer URLs, and viewed pages. It is also designed to capture click events and conversion actions—such as form submissions or account sign-ups on the Website. Through the use of cookies and unique identifiers, the Bing / Microsoft Ads Tracker can track users across sessions and websites to build behavioral profiles and deliver targeted advertising.

86. ***Figure 5*** below is a screenshot from the Website showing a network request to bat.bing.com, confirming that the Microsoft Bing Ads Tracker was triggered automatically upon page load. The request loaded the Bing Ads script without any user interaction, indicating that Microsoft's tracking infrastructure was activated in the background. This network activity occurred without notice or consent, demonstrating that user data was transmitted to Microsoft's tracking servers immediately upon visiting the homepage.

/ /

/ /

/ /

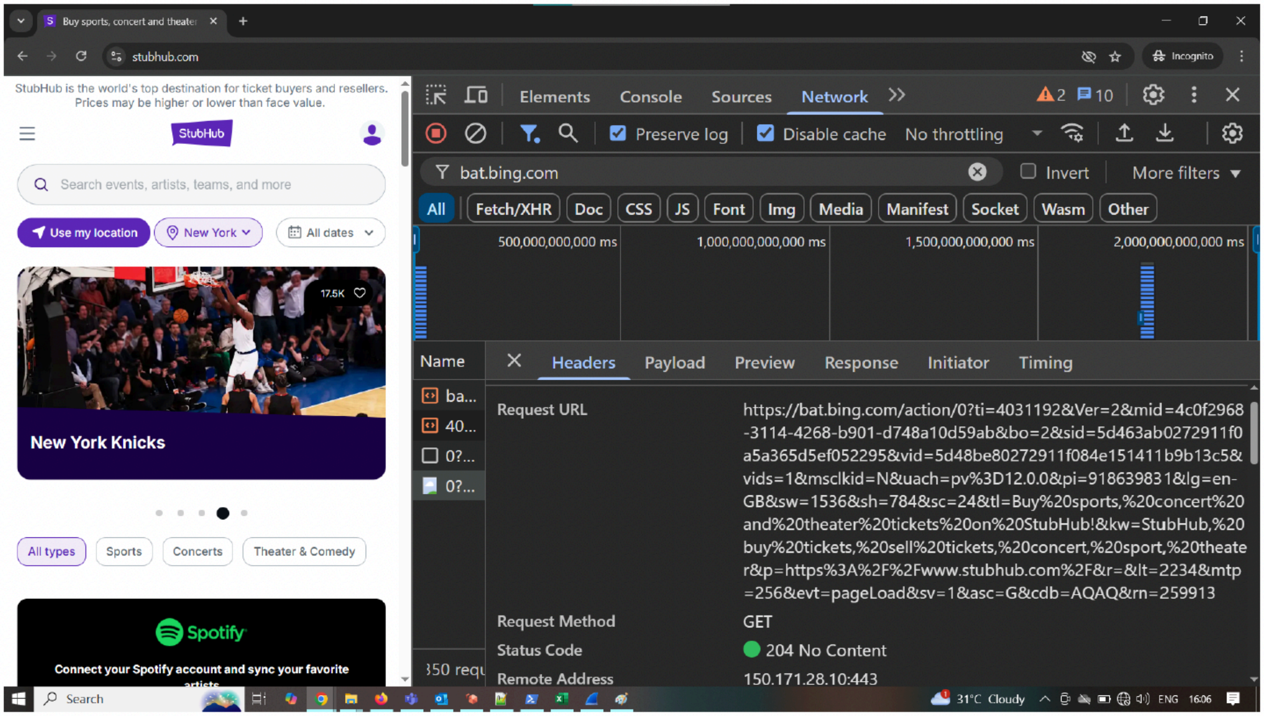
/ /

/ /

/ /

/ /

Figure 5



Filter: bat.bing.com

Request URL: https://bat.bing.com/action/0?ti=4031192&Ver=2&mid=4c0f2968-3114-4268-b901-d748a10d59ab&bo=2&sid=5d463ab0272911f0a5a365d5ef052295&vid=5d48be80272911f084e151411b9b13c5&vids=1&msclkid=N&uach=pv%3D12.0.0&pi=918639831&lg=en-GB&sw=1536&sh=784&sc=24&tl=Buy%20sports,%20concert%20and%20theater%20tickets%20on%20StubHub!&kw=StubHub,%20buy%20tickets,%20sell%20tickets,%20concert,%20sport,%20theater&p=https%3A%2F%2Fwww.stubhub.com%2F&r=&lt=2234&mtp=256&evt=pageLoad&sv=1&asc=G&cdb=AQAQ&rn=259913

Request Method: GET

Status Code: ● 204 No Content

Remote Address: 150.171.28.10:443

87. *Figure 6* below captures the payload data transmitted to bat.bing.com, confirming that the Bing / Microsoft Ads Tracker sends detailed metadata to third-party ad servers during the user's session. The payload includes the referrer URL, session context, and unique identifiers associated with the user's browsing activity. This transmission occurs automatically upon page load, without any user interaction or consent. The presence of this behavioral data in the payload confirms that StubHub shares session-level information with Microsoft's advertising infrastructure for tracking and targeting purposes.

/ /

/ /

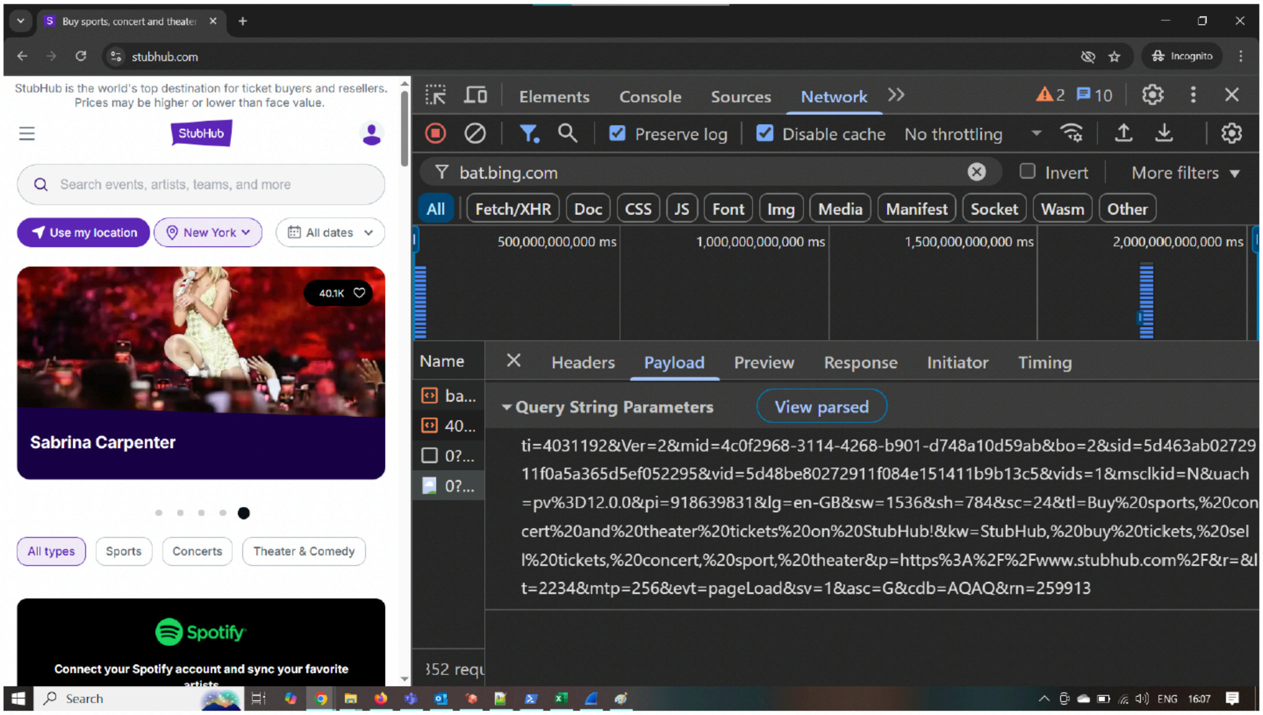
/ /

/ /

/ /

/ /

Figure 6



StubHub is the world's top destination for ticket buyers and resellers. Prices may be higher or lower than face value.

▾ Query String Parameters   View parsed

```
ti=4031192&Ver=2&mid=4c0f2968-3114-4268-b901-d748a10d59ab&bo=2&sid=5d463ab02729
11f0a5a365d5ef052295&vid=5d48be80272911f084e151411b9b13c5&vids=1&msclkid=N&uach
=pv%3D12.0.0&pi=918639831&lg=en-GB&sw=1536&sh=784&sc=24&tl=Buy%20sports,%20con
cert%20and%20theater%20tickets%20on%20StubHub!&kw=StubHub,%20buy%20tickets,%20sel
l%20tickets,%20concert,%20sport,%20theater&p=https%3A%2F%2Fwww.stubhub.com%2F&r=&l
t=2234&mtp=256&evt=pageLoad&sv=1&asc=G&cdb=AQAQ&rn=259913
```

88. *Figure 7* below shows DNS resolution activity to bat.bing.com, confirming that the Website initiated communication with Microsoft's tracking infrastructure during the initial session. This DNS request occurred as part of the automatic activation of the Bing / Microsoft Ads Tracker and was initiated without any user interaction or awareness. The evidence demonstrates that STUBHUB began communicating with Microsoft's tracking services at the DNS level immediately upon page load, without disclosing this behavior to the user or providing an opportunity to opt out.

/ /

/ /

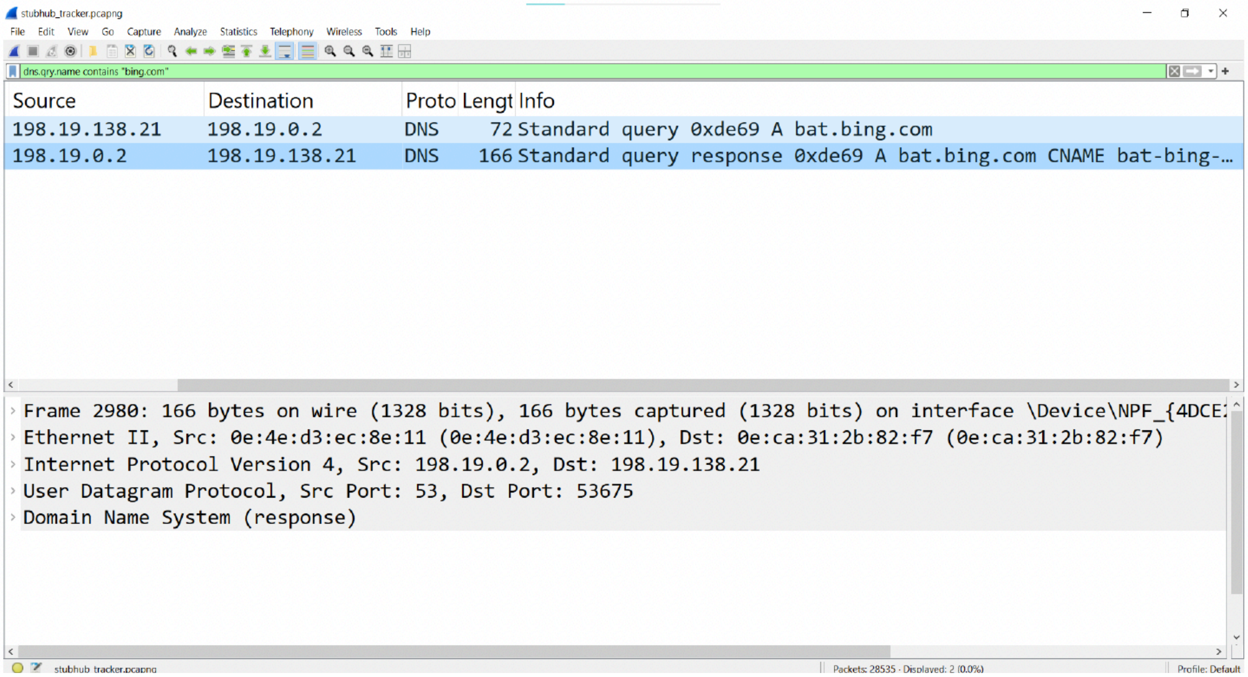
/ /

/ /

/ /

/ /

Figure 7


stubhub_tracker.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "bing.com"

Source	Destination	Proto	Lengt	Info
198.19.138.21	198.19.0.2	DNS	72	Standard query 0xde69 A bat.bing.com
198.19.0.2	198.19.138.21	DNS	166	Standard query response 0xde69 A bat.bing.com CNAME bat-bing-…

```
› Frame 2980: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface \Device\NPF_{4DCE:
› Ethernet II, Src: 0e:4e:d3:ec:8e:11 (0e:4e:d3:ec:8e:11), Dst: 0e:ca:31:2b:82:f7 (0e:ca:31:2b:82:f7)
› Internet Protocol Version 4, Src: 198.19.0.2, Dst: 198.19.138.21
› User Datagram Protocol, Src Port: 53, Dst Port: 53675
› Domain Name System (response)
```

89. Defendant surreptitiously installed, executed, and embedded the Bing / Microsoft Ads Tracker onto users' browsers by including Microsoft's JavaScript tracking code directly in the Website's source code. When a user visits the Website, their browser executes this code, which triggers outbound requests to Microsoft's servers and transmits metadata including the user's IP address, page URL, referrer, and session-specific identifiers.

90. The Bing / Microsoft Ads Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data.

91. The Bing / Microsoft Ads Tracker is at least a "device" because in order for software to work, it must be run on some kind of computing device. See, e.g., *James v. Walt Disney Co.* 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

92. The Bing / Microsoft Ads Tracker initiates a connection to its ad infrastructure upon page load via a script or pixel execution. It captures user metadata such as IP address, page path, timestamp, and unique identifiers - all of which qualify as routing or signaling information under CIPA.

/ /

93. The Bing / Microsoft Ads Tracker collects real-time signaling and routing information from the user's device without direct interaction. It acts as a pen register by capturing outbound metadata such as page visits, click events, and form submissions, and as a trap and trace device by receiving inbound responses like ad content and tracking pixels. These communications occur passively, enabling Microsoft to assign user identifiers, build behavior profiles, and facilitate personalized advertising, all without the user's knowledge or consent.

94. Defendant never obtained a court order permitting the installation of a pen register or trap and trace device or process and did not obtain Plaintiff's or the Class Members' express or implied consent to install the Bing / Microsoft Ads Tracker on Plaintiff's and Class Members' browser or to collect or share data with Microsoft.

95. Consequently, the Bing / Microsoft Ads Tracker violates CIPA regarding unauthorized use of a pen register and/or trap and trace device without prior consent or court order.

3. The Branch.io Tracker

96. The Branch.io Tracker, loaded from domains controlled by Branch Metrics Inc., is a third-party tracking technology designed to support cross-platform attribution and behavioral analytics. On the Website, this tracker is dynamically injected into the user's browser during the initial session. Upon activation, the Branch.io Tracker initiates communication with Branch's servers and collects various data points, including IP address, device information, browser version, session context, and unique identifiers such as device IDs or referral codes. These transmissions occur automatically in the background, without any user interaction or consent, confirming that user activity is being monitored in real time for attribution, engagement tracking, and behavioral segmentation.

97. Once active, the Branch.io Tracker plays a key role in identity resolution by assigning persistent identifiers that can be associated with users across different sessions, devices, and platforms. This is achieved using techniques such as deep link

attribution, fingerprinting, and tracking referral paths. These capabilities allow Branch.io to link activity on the Website with broader user journeys across apps and mobile environments, effectively stitching together a user’s interactions even when they do not log in. This functionality supports the construction of unified user profiles based on behavior across channels.

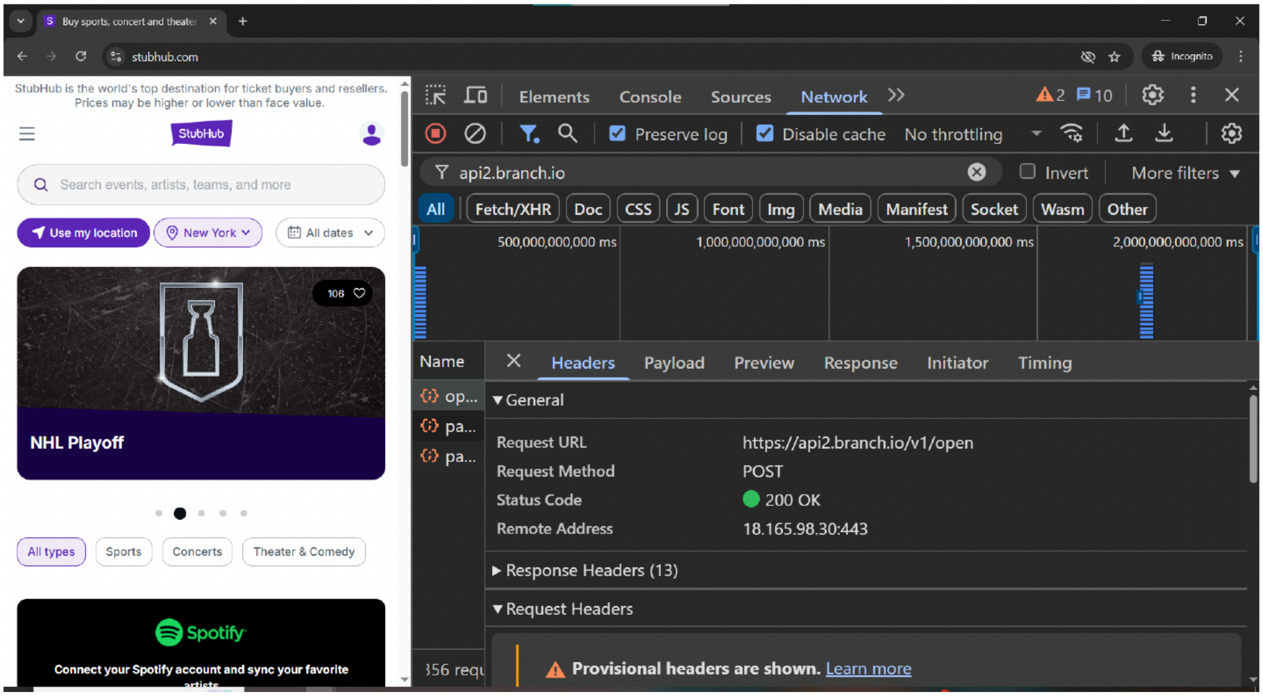
98. The Branch.io Tracker enables STUBHUB to carry out targeted marketing efforts by tracking users who enter the Website via specific campaigns, links, or referring sources. STUBHUB can then use this information to retarget users with customized messaging based on their interaction history, both on and off the Website. Branch.io’s attribution and segmentation tools allow STUBHUB to analyze user intent, optimize advertising spend, and build lookalike audiences composed of users who exhibit similar behavioral characteristics. These features enhance STUBHUB’s ability to re-engage visitors and attract new users with tailored campaigns that align with their marketing objectives.

99. On the Website, the Branch.io Tracker transforms real-time user interactions into valuable behavioral data that STUBHUB leverages for campaign optimization and revenue generation. By capturing detailed engagement signals and associating them with referral sources and session outcomes, Branch.io helps STUBHUB measure the effectiveness of marketing efforts and identify high-performing audience segments. This data feeds into performance analytics and attribution models that inform STUBHUB’s broader digital marketing strategy. Through these mechanisms, Branch.io enables STUBHUB to monetize user behavior, refine targeting, and support data-driven decision making across its marketing operations.

100. ***Figure 7*** below an outbound request is made to api2.branch.io/v1/open immediately upon loading the Website. This request, captured during the initial session, confirms that the Branch.io Tracker is activated without any user interaction. The presence of this call indicates that STUBHUB initiates

attribution tracking through Branch.io at the moment the Website loads, transmitting user metadata such as device context and referral information before any consent is provided. This behavior demonstrates that Branch.io's tracking infrastructure is engaged by default and begins collecting data from users without prior notice or opt-in.

Figure 7



☑ Preserve log ☑ Disable cache No throttling

Filter: api2.branch.io

▼ General

Request URL https://api2.branch.io/v1/open

Request Method POST

Status Code ● 200 OK

Remote Address 18.165.98.30:443

▶ Response Headers (13)

▼ Request Headers

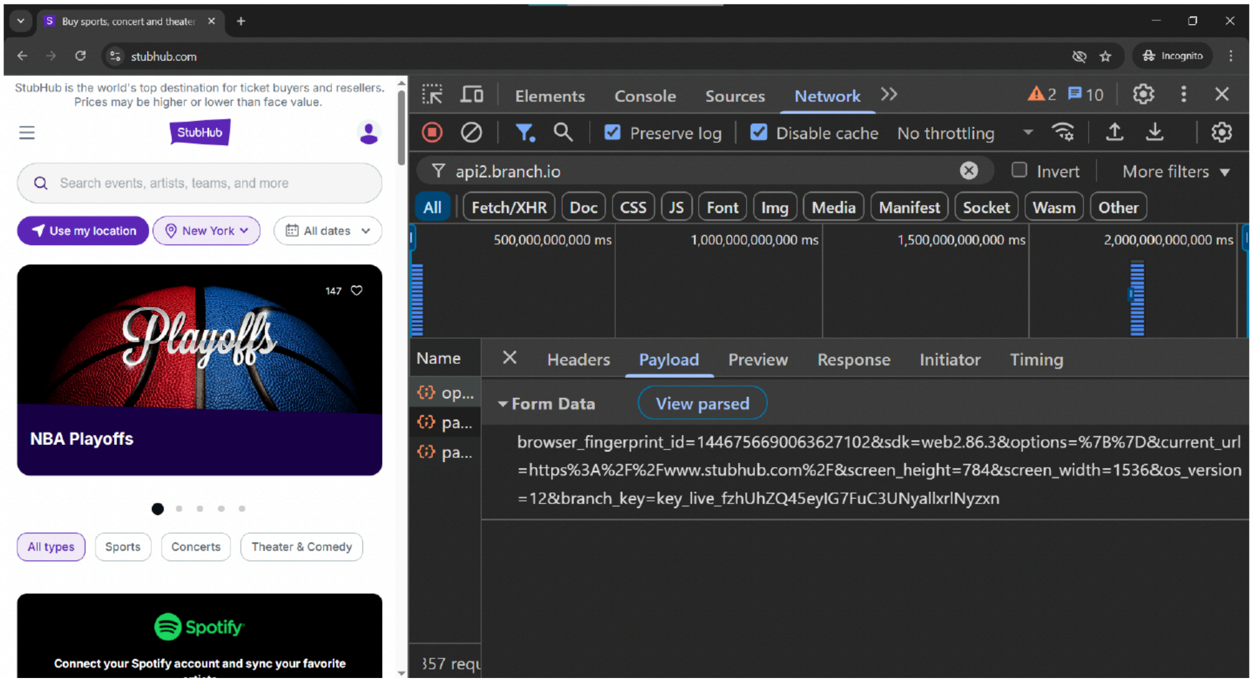
⚠ Provisional headers are shown. Learn more

101. ***Figure 8*** below shows payload data transmitted to api2.branch.io confirms that the Branch.io Tracker collects and sends detailed fingerprinting information as soon as the Website loads. The payload includes browser metadata, referrer URLs, device identifiers, and other contextual information used to uniquely identify users and attribute sessions. This data is transmitted automatically, without any user interaction or consent. The presence of this information in the outbound request demonstrates that STUBHUB enables Branch.io to perform user tracking and session attribution from the outset, allowing the collection of identifiable data prior to any opportunity for the user to opt in or manage their privacy preferences.

/ /

/ /

Figure 8



```
browser_fingerprint_id=1446756690063627102&sdk=web2.86.3&options=%7B%7D&current_url
=https%3A%2F%2Fwww.stubhub.com%2F&screen_height=784&screen_width=1536&os_version
=12&branch_key=key_live_fzhUhZQ45eylG7FuC3UNyallxrlNyzxn
```

102. Defendant surreptitiously installed, executed, embedded, or injected the Branch.io Tracker onto users' browsers by deploying JavaScript code that triggers communication with Branch.io's tracking infrastructure. When a user visits the Website, their browser automatically executes this code, initiating outbound requests to Branch.io's servers and transmitting user metadata, including IP address, referrer URL, device type, browser characteristics, and other unique identifiers. This transmission occurs silently and without any user action, enabling Branch.io to capture data about user sessions and behaviors on the Website in real time.

103. The Branch.io Tracker is at least a "process" because it is software that identifies consumers, gathers data, and correlates that data across websites, sessions, and devices for attribution and user profiling.

104. The Branch.io Tracker is at least a "device" because, in order for software to operate, it must be executed on a computing device such as a smartphone, laptop, or desktop browser. See, e.g., *James v. Walt Disney Co.*, 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

/ /

105. The Branch.io Tracker initiates a connection to its attribution infrastructure upon page load via script execution. It captures user metadata such as IP address, referrer URL, timestamp, browser type, and device identifiers, each of which qualifies as routing, addressing, or signaling information.

106. The user does not intentionally initiate any communication with Branch.io; rather, the connection is triggered automatically and invisibly in the background by embedded third-party code on the Website. As a result, Branch.io is able to silently intercept and record communication-related data generated during the user's visit. In this manner, the Branch.io Tracker functions as a surveillance mechanism that captures third-party signaling information without the user's awareness.

107. Defendant never obtained a court order authorizing the use of a pen register or trap and trace process, nor did Defendant obtain Plaintiff's or the Class Members' express or implied consent to install the Branch.io Tracker on their browsers or to transmit metadata to Branch.io.

108. Accordingly, the installation and operation of the Branch.io Tracker on the Website constitutes a violation of CIPA, specifically with respect to the unauthorized use of a pen register and/or trap and trace device or process without the required legal authority or prior consent.

4. The Viagogo Tracker

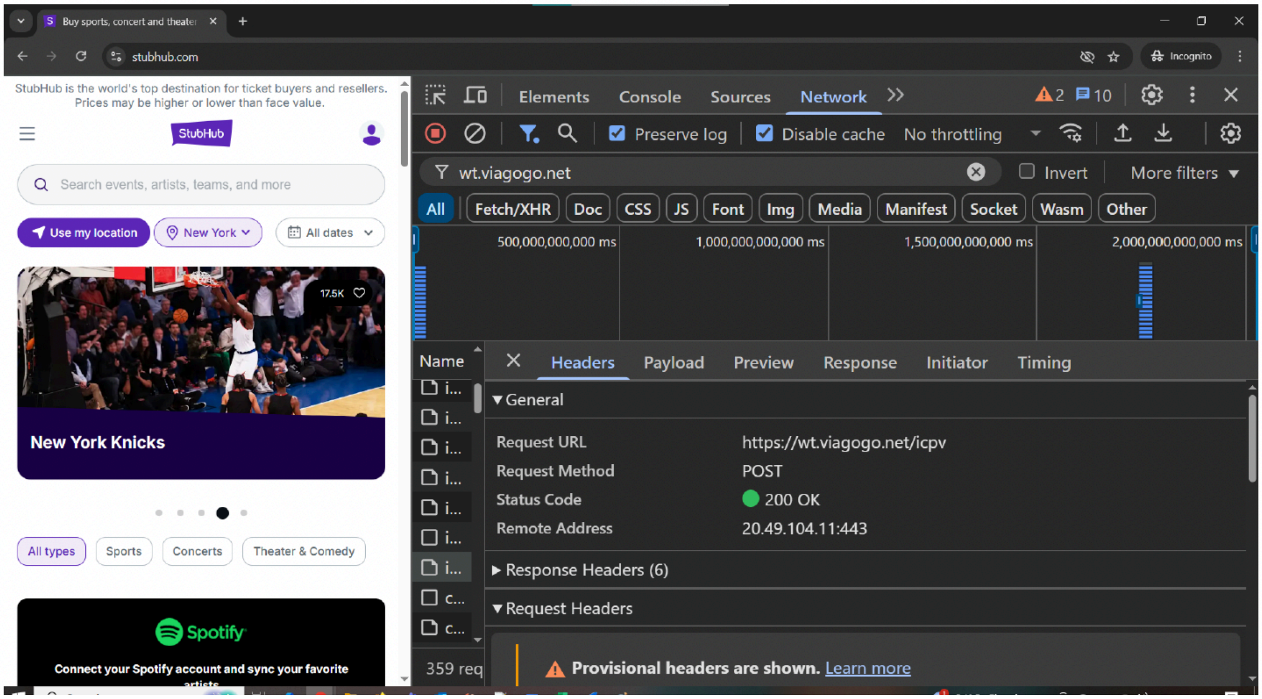
109. The Viagogo Tracker is a cross-platform tracking and attribution tool used to monitor user behavior, session metadata, and browsing patterns across affiliated properties. When deployed, the Viagogo Tracker collects data such as page views, referral sources, timestamps, IP addresses, device and browser details, and navigation paths. On the Website, the Viagogo Tracker was active during the session and began collecting tracking data automatically upon page load, without any user interaction or consent.

110. By capturing both behavioral and technical data, the Viagogo Tracker enables StubHub to conduct session analysis, behavioral segmentation, and user

targeting across related platforms. This functionality allows StubHub to link on-site user activity with broader engagement profiles maintained by Viagogo, supporting identity resolution, retargeting, and marketing personalization. The data collected by the Viagogo Tracker facilitates both audience enrichment and data monetization by helping StubHub identify high-value users and optimize outreach strategies across multiple channels.

111. ***Figure 9*** below is a screenshot from the Website confirming that a POST request to wt.viagogo.net/icpv is initiated instantly upon loading the Website. This request receives a 200 status code and is directed to IP address 20.49.104.11, indicating a successful connection to Viagogo's tracking infrastructure. The request occurs automatically during the initial session, without any user interaction, confirming that the Viagogo Tracker is activated silently on page load. This behavior demonstrates that StubHub transmits user data to Viagogo's third-party servers by default, establishing a tracking relationship without user notice or consent.

Figure 9



StubHub is the world's top destination for ticket buyers and resellers. Prices may be higher or lower than face value.

☑ Preserve log ☑ Disable cache No throttling

wt.viagogo.net □ Invert

▾General

Request URL https://wt.viagogo.net/icpv

Request Method POST

Status Code ● 200 OK

Remote Address 20.49.104.11:443

▸Response Headers (6)

▾Request Headers

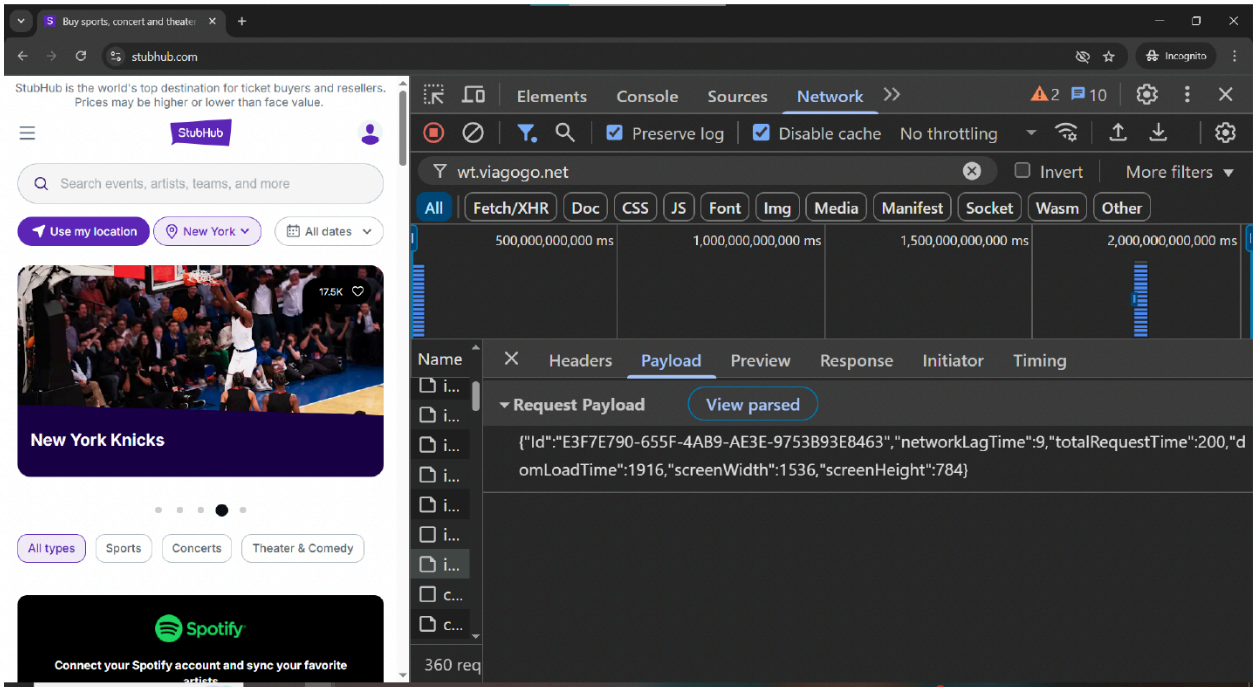
⚠ Provisional headers are shown. Learn more

Connect your Spotify account and sync your favorite artists

//

112. ***Figure 10*** below shows payload data sent to wt.viagogo.net reveals that the Viagogo Tracker transmits detailed session-level information to third-party servers. The JSON payload includes a unique user ID, screen resolution, total request time, and page load time, data points that allow Viagogo to identify individual users and monitor their browsing experience in real time. This information is sent automatically upon page load, without any user action or consent. The presence of uniquely identifying and performance-related data in the payload confirms that StubHub shares sensitive session data with Viagogo's tracking infrastructure by default, enabling user profiling without transparency or opt-in.

Figure 10

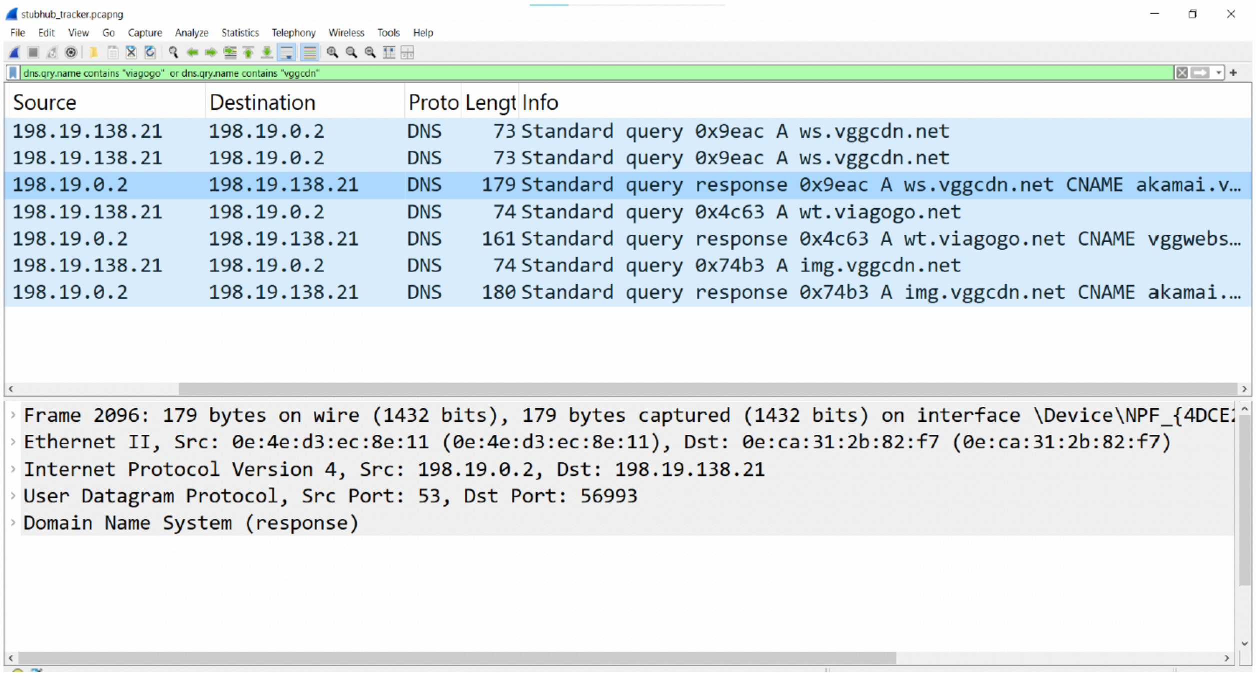


{"Id":"E3F7E790-655F-4AB9-AE3E-9753B93E8463","networkLagTime":9,"totalRequestTime":200,"domLoadTime":1916,"screenWidth":1536,"screenHeight":784}

113. ***Figure 11*** below captures DNS logs that show that the Website initiates backend communication with multiple Viagogo-affiliated domains, including wt.viagogo.net, img.vggcdn.net, and ws.vggcdn.net, during the initial session. These DNS queries confirm that server-level tracker components are being loaded automatically as part of the page initialization process. The resolution of these domains occurs before the user has any opportunity to opt in or opt out of data collection, indicating that StubHub establishes communication with Viagogo's tracking

infrastructure in the background without user awareness or consent. This activity supports the conclusion that tracking is embedded at the system level and activated by default.

Figure 11



stubhub_tracker.pcapng

dns.qry.name contains "viagogo" or dns.qry.name contains "vggcdn"

```
Source          Destination     Proto Lengt Info
198.19.138.21   198.19.0.2      DNS      73 Standard query 0x9eac A ws.vggcdn.net
198.19.138.21   198.19.0.2      DNS      73 Standard query 0x9eac A ws.vggcdn.net
198.19.0.2      198.19.138.21   DNS     179 Standard query response 0x9eac A ws.vggcdn.net CNAME akamai.v…
198.19.138.21   198.19.0.2      DNS      74 Standard query 0x4c63 A wt.viagogo.net
198.19.0.2      198.19.138.21   DNS     161 Standard query response 0x4c63 A wt.viagogo.net CNAME vggwebs…
198.19.138.21   198.19.0.2      DNS      74 Standard query 0x74b3 A img.vggcdn.net
198.19.0.2      198.19.138.21   DNS     180 Standard query response 0x74b3 A img.vggcdn.net CNAME akamai.…
```

```
› Frame 2096: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface \Device\NPF_{4DCE
› Ethernet II, Src: 0e:4e:d3:ec:8e:11 (0e:4e:d3:ec:8e:11), Dst: 0e:ca:31:2b:82:f7 (0e:ca:31:2b:82:f7)
› Internet Protocol Version 4, Src: 198.19.0.2, Dst: 198.19.138.21
› User Datagram Protocol, Src Port: 53, Dst Port: 56993
› Domain Name System (response)
```

114. Defendant surreptitiously installed, executed, or injected the Viagogo Tracker onto users' browsers by triggering Viagogo's JavaScript-based tracking code during page load. When a user visits the Website, their browser automatically executes this script, which transmits data about the user's session, including IP address, page URL, screen resolution, and other behavioral metadata, to Viagogo's servers. This transmission occurs in the background, without the user's awareness or interaction, confirming the tracker operates silently upon entry.

115. The Viagogo Tracker is at least a "process" because it is software that identifies consumers, collects behavioral data, and correlates that data for tracking and profiling purposes.

116. The Viagogo Tracker is at least a "device" because it functions through execution on computing devices such as desktop browsers or mobile phones. See, e.g., *James v. Walt Disney Co.*, 2023 WL 7392285 at *13 (N.D. Cal. Nov. 8, 2023).

117. The Viagogo Tracker captures non-content signaling information including IP addresses, visited URLs, timestamps, referrer data, screen resolution, and browser or device identifiers. This metadata relates to the routing and addressing components of the user's electronic communications with the Website and is used to establish and monitor ongoing sessions.

118. Viagogo conducts user tracking and behavioral profiling without the user's knowledge or consent by collecting and processing granular session data through STUBHUB's Website. This tracking includes timing, navigation, and environment-related data that can be used to analyze behavior in real time.

119. The persistent identifiers used by Viagogo enable it to monitor user behavior across multiple browsing sessions and contexts. This allows STUBHUB, through Viagogo's infrastructure, to construct detailed user profiles and apply those insights to advertising, engagement, and monetization strategies, all without user awareness or consent.

120. The Viagogo Tracker initiates a connection to Viagogo-controlled servers, such as wt.viagogo.net, ws.vggcdn.net, and img.vggcdn.net, immediately upon page load. These requests transmit routing and signaling metadata, including the user's IP address, user-agent string, full URL path, screen and device attributes, referrer header, and timestamps. These data points allow Viagogo to identify both the source and destination of the user's electronic communication, making the tracker function as a pen register and/or trap and trace device or process.

121. Defendant never obtained a court order authorizing the use of a pen register or trap and trace device or process, and did not obtain the express or implied consent of Plaintiff or the Class Members to install the Viagogo Tracker or to transmit data to Viagogo.

122. Accordingly, Defendant's undisclosed installation and operation of the Viagogo Tracker on the Website constitutes a violation of CIPA, specifically concerning the unauthorized use of a pen register and/or trap and trace device or process

without lawful consent or judicial approval.

VI. CLASS ALLEGATIONS

123. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class" or "Class Members") defined as follows:

> All persons within California whose browser was subject to installation, execution, embedding, or injection of the Trackers by the Defendant's Website during the relevant statute of limitations period.

124. **NUMEROSITY:** Plaintiff does not know the number of Class Members but believes the number to be in the thousands, if not more. The exact identities of Class Members can be ascertained by the records maintained by Defendant.

125. **COMMONALITY:** Common questions of fact and law exist as to all Class Members and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class Member, include but are not limited to the following:

- Whether Defendant installed, executed, embedded or injected the Trackers on the Website;
- Whether the Trackers are each a pen register and/or trap and trace device as defined by law;
- Whether Plaintiff and Class Members are subject to same tracking policies and practices;
- Whether Plaintiff and Class Members are entitled to statutory damages;
- Whether Class Members are entitled to injunctive relief;
- Whether Class Members are entitled to disgorgement of data unlawfully obtained;
- Whether the Defendant's conduct violates CIPA; and
- Whether the Defendant's conduct constitutes an unlawful, misleading,

deceptive or fraudulent business practice.

126. **TYPICALITY:** As a person who visited Defendant's Website and whose outgoing electronic information was surreptitiously collected by the Trackers, Plaintiff is asserting claims that are typical of the Class Members. Plaintiff's experience with the Trackers is typical to Class Members.

127. **ADEQUACY:** Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained attorneys experienced in class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the Class or whose inclusion would otherwise be improper are excluded.

128. **SUPERIORITY:** A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class Members is impracticable and inefficient. Even if every Class Member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

VII. FIRST CAUSE OF ACTION

Violations of Cal. Penal Code § 638.51

By Plaintiff and the Class Members Against All Defendants

129. Plaintiff reasserts and incorporates by reference the allegations set forth in each preceding paragraph as though fully set forth herein.

130. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

131. Defendant uses a pen register device or process and/or a trap and trace device or process on its Website by deploying the Trackers because the Trackers are designed to capture the IP address, User Information and other information such as the phone number, email, routing, addressing and/or other signaling information of website visitors.

/ /

132. Defendant did not obtain consent from Plaintiff or any of the Class Members before using pen registers or trap and trace devices to locate or identify users of its Website and has thus violated CIPA. CIPA imposes civil liability and statutory penalties for violations of § 638.51. Cal. Penal Code § 637.2; *Moody v. C2 Educational Systems, Inc.*, No. 2:24-cv-04249-RGK-SK, 2024 U.S. Dist. LEXIS 132614 (C.D. Cal. July 25, 2024).

VIII. <u>SECOND CAUSE OF ACTION</u>

Violations of Business & Professions Code § 17200

By Plaintiff and the Class Members Against All Defendants

133. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Complaint as though fully set forth herein.

134. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendant.

135. This cause of action is brought under California Business & Professions Code § 17200 et seq., which prohibits any unlawful, unfair, or fraudulent business act or practice.

136. Defendant has engaged in unlawful business practices by:

(a) Violating California Penal Code §§ 638.50–638.56, including the unauthorized collection of addressing, signaling, and routing information for user identification and tracking; and

(b) Violating California Civil Code § 1798.100, *et seq.*, including collecting, using, and/or selling Plaintiff's and Class Members' personal information and location data to Third Parties without providing sufficient notice. Privacy rights rooted in the CCPA are a protected interest enforceable under Business & Professions Code § 17200. *Briskin v. Shopify, Inc.*, 101 F.4th 706 (9th Cir. 2025) (en banc).

137. Defendant has engaged in unfair business practices by embedding the Trackers into the Website and enabling the real-time capture and transmission of Plaintiff's and Class Members' personal and behavioral information, such as IP address,

browser details, visited URLs, referrer paths, timestamps, and interaction events, to the Third Parties.

138. The Defendant's practices are contrary to public policy supporting consumer privacy and data autonomy, and the harm it causes to consumers, including loss of control over personal information and risk of profiling, outweighs any legitimate business justification.

139. Defendant has engaged in fraudulent business practices by failing to adequately disclose its data-sharing practices. On information and belief, Defendant omitted material facts from its privacy policy and/or site interface and failed to inform users that their activities would be tracked across the internet and linked to unique identifiers for advertising and profiling purposes. These omissions were likely to deceive a reasonable consumer and were intended to obscure the nature and extent of the surveillance.

140. As a direct and proximate result of Defendant's unlawful, unfair, and fraudulent conduct, Plaintiff and the Class Members have suffered injury in fact and loss of money or property, including the unauthorized exfiltration and commodification of valuable personal data. Plaintiff's and Class Members' data—used for targeted advertising, behavioral modeling, and enrichment by third parties—constitutes digital property with measurable economic value.

141. Plaintiff on behalf of himself and on behalf of the Class Members seeks injunctive relief to prevent Defendant from continuing its deceptive and unlawful data tracking practices and to require clear and conspicuous notice and opt-in consent for any behavioral tracking involving third-party tools. Plaintiff on behalf of himself and on behalf of the Class Members, also seeks restitution of the value derived from the unauthorized use of their personal information, attorneys' fees where permitted by law, and such other and further relief as the Court may deem just and proper.

/ /

/ /

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following:

1. An order certifying the Class, naming Plaintiff as Class representative, and naming Plaintiff's attorneys as Class counsel;
2. An order declaring that Defendant's conduct violates CIPA and Business & Professions Code § 17200;
3. An order of judgment in favor of Plaintiff and the Class against Defendant on the causes of action asserted herein;
4. An order enjoining Defendant's conduct as alleged herein;
5. Statutory damages pursuant to CIPA;
6. Prejudgment interest;
7. Reasonable attorney's fees and costs; and
8. All other relief that would be just and proper as a matter of law or equity.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so permitted.

Dated: July 21, 2025 **NATHAN & ASSOCIATES, APC**

By: /s/ Reuben D. Nathan
Reuben D. Nathan, Esq.
Attorneys for Plaintiff